Next Steps for Deploying a National Security Credential Management System for V2X Communications

SAE Government Industry Meeting

Washington, DC

January 25th, 2018

NHTSA

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Motivation for SCMS

Connected vehicles have the potential to transform the way Americans travel through the creation of a safe, interoperable wireless communications network.

- **V2X safety applications** can alert the driver and help prevent crashes by issuing safety warnings.
- V2X can support **automated vehicle operations and safety**

To realize the benefits of V2X, messages need to be trusted:

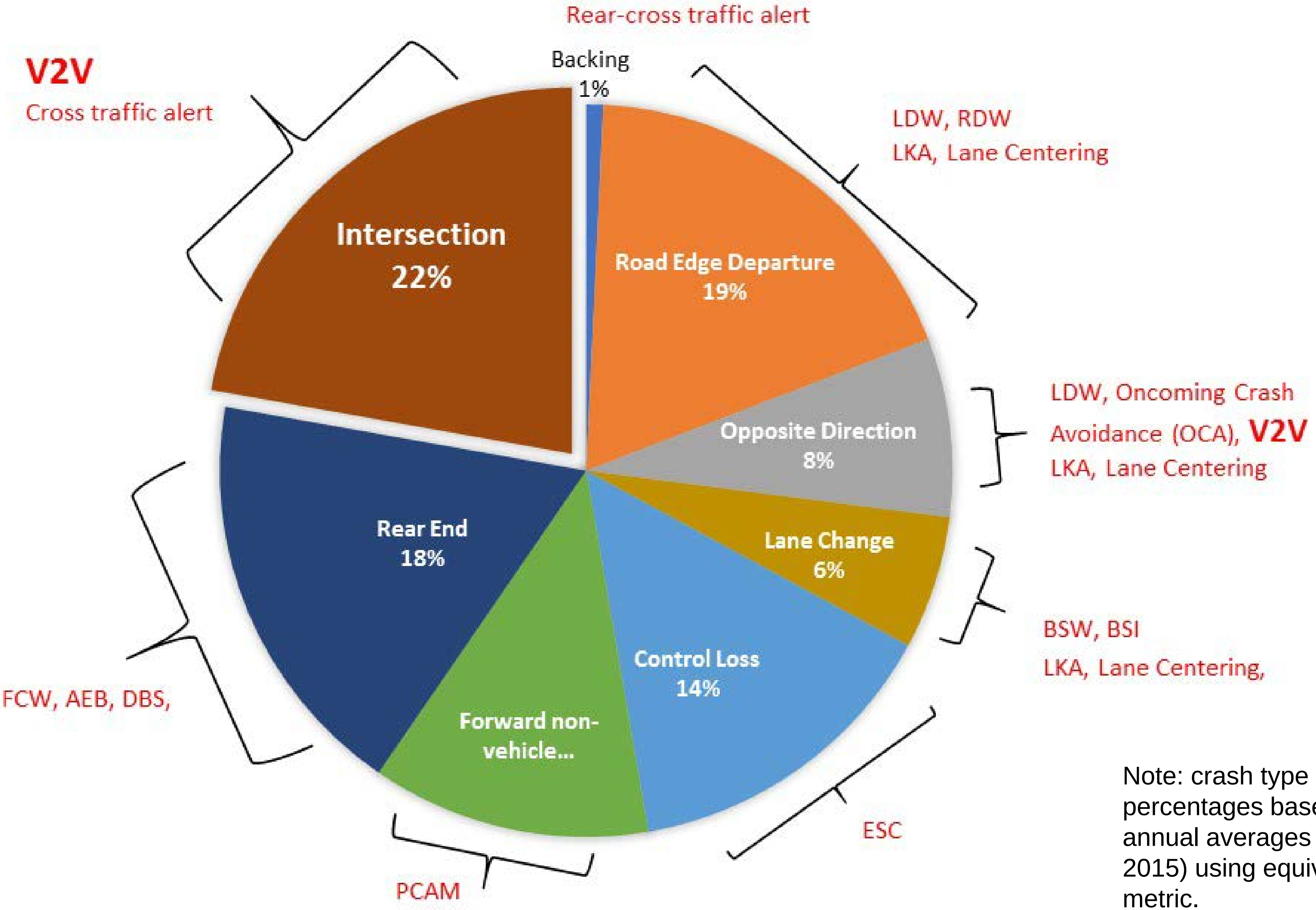
Integrity – the message was not modified between sender and receiver

Authenticity – the message originates from a trustworthy and legitimate device

Privacy – the message appropriately protects the privacy of the sender

Situations Highlighting Opportunities

Crash types mapped to ADAS countermeasures



Note: crash type percentages based on annual averages (2011 to 2015) using equivalent lives metric.

Where are we at with SCMS Development?

- **Mostly done….but some missing elements**
  - Electors concept
  - Re-enrollment capability
  - Local and global misbehavior integration
  - Other “tweaks”
- **Prototype has been built and is being demonstrated**
  - Demonstrated scalability using modeling and simulation
  - Real-world testing via servicing of Federally-funded deployments
- **Some early analysis and outreach efforts on how to deploy at scale (nationally)**
  - Cost models developed (CAMP and BAH) for various infrastructure deployment scenarios.
  - High-level ideas on Governance, Operations, Management and funding developed by the Vehicle Infrastructure Integration Consortium (VIIC)
  - Responses to NHTSA Request for Information on SCMS deployment in 2014

Where do we need to be....and by when?

- **Certificate management services are being requested now!**
  - OEM product offerings
  - ASD Suppliers
  - Infrastructure deployer's (States, RSU suppliers)

- **PKI service providers are willing and able to "step up"....but,**

- **As Security Credential Management Services are deployed nationally, how are key public and private objectives accomplished?**
  - Privacy
  - Trust maintenance (integrity and authenticity of messages)
  - Cost control and cost realism (competition)
  - Interoperability
  - Availability (to various end-entities)

Numerous Technical and Policy Challenges…examples:

- **Enrollment of users into the system**
  - Authorizing users (certification and compliance requirements)
  - Enrollment (secure processes in place that can be audited)
  - And Re-enrollment
- **Root Management**
  - Single versus multiple roots
  - Root electors
  - Root retirement
- **Global Misbehavior Detection**
  - Efficiency versus privacy
  - Criteria for revocation
  - Auditing and transparency
- **Local Misbehavior Detection**

And there are key organizational challenges..

- Stakeholder representation
- Funding and Business Models
- Sustainability and recovery plans
- Oversight and Auditing
- Dispute resolution
- Management of Trust Anchors
- Privacy
- Interoperability

….Developing an overall SCMC eco-system Governance and Management solution is key

SCMS Governance & Management research…

- **USDOT wishes to work with all impacted stakeholders to develop, and implement, viable pathways toward large scale deployment of an SCMS eco-system.**
- **Have retained a consultant to help manage industry outreach activities**
- **Key tasks include:**
  - Documenting what we know now about needs, functionality, and designs related to the SCMS (to help with interactions with stakeholders)
  - Document V2X security system approaches (including Governance) in other international markets
  - Identify large PKI system deployments from other industries or sectors that may provide possible parallels
  - **Research potential Governance, Ownership and Management Models**
  - Interview PKI experts and stakeholder groups to gather feedback, modify models, or develop alternative models
  - Conduct table-top exercises and workshops to further define potential paths forward—and to define specific next steps for industry and government.

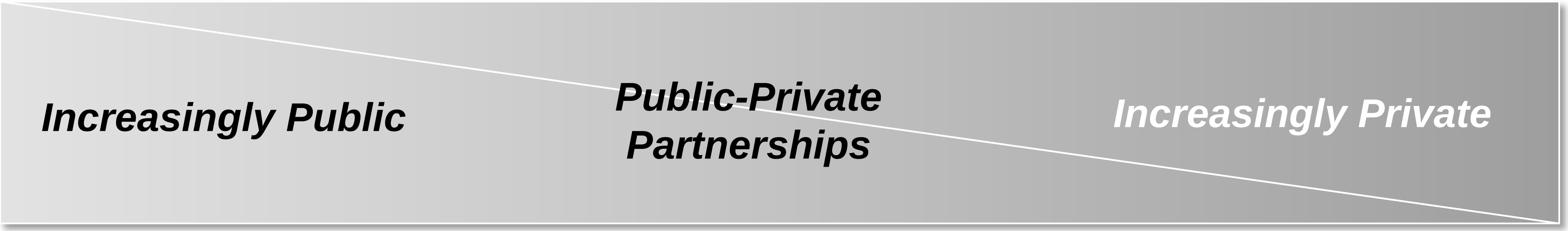
Scoping Model Development ….

Example considerations and assumptions:

1. a multiple Root CA structure
2. the Misbehavior Authority is a centralized and stand-alone function.
3. one entity or organization cannot operate every aspect within the SCMS ecosystem
   a) Separation of SCMS operational entities and functions to maintain security and privacy, but also to enhance flexibility, competitiveness and resiliency
4. Interoperability, privacy, operational sustainment (redundantcy) and cost realism are imperatives

Scoping Model Development ....

There exists a range of SCMS Management, ownership and governance models based on the desired (and potentially necessary) public and private involvement…



- Ownership
- Funding
- Policy Creation and Approval (incl. interoperability reqts.)
- Oversight and Auditing
- Trust Anchor Management
- Certification of devices
- Operation of inherently central components

Models will be evaluated against key criteria…

	Public				Private
Security					
Privacy					
Availability (Interoperability flexibility)					
Stakeholder Representation					
Affordability					
Performance					
Robustness (Sustainability, Redundancy)					
Other?					

You are invited to help!

- **Stay tuned for info about future public meetings, interviews and related efforts.**
- **For more information, contact:**

Robert Kreeb (NHTSA)
Robert.kreeb@dot.gov
202 366 0587